# Integrating Innovation

## Keeping the Leading Edge

*Kevin Fahey*

From the Jeep to the Internet to GPS, there was a time when the U.S. military led the way in inventing technologies that would later become dominant in the general public.

Times have changed. Today, we more often see the opposite pattern—the commercial sector achieves the breakthrough, and the military adopts and adapts it to meet our requirements.

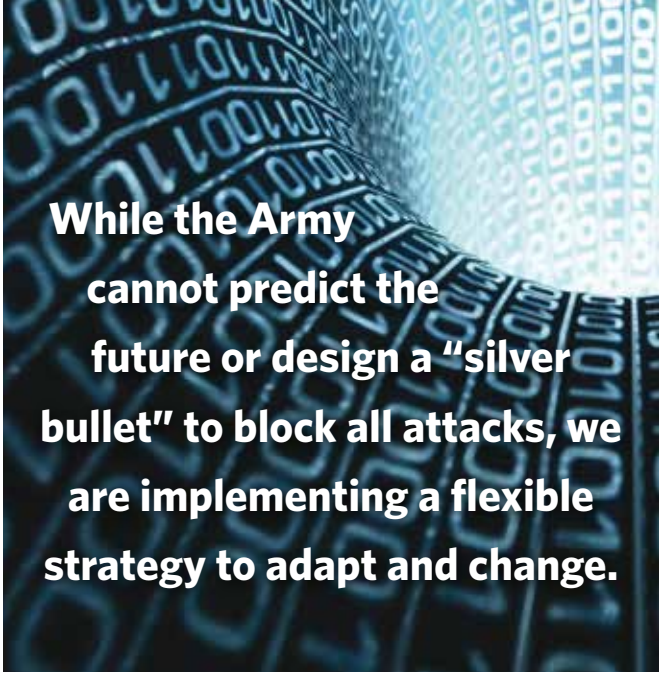
This reality means that our adversaries have access to many of the same technologies in the commercial marketplace that we do—without the hurdles that exist in our acquisition system. To maintain our superiority, our acquisition approach must be adaptive enough to enable rapid technology insertion, but also disciplined enough to ensure holistic interoperability once the systems are in warfighters' hands. Put simply, our challenge is to be the integrator among fast-moving innovators.

That framework is driving today's efforts in the Army acquisition community to set conditions for future success. Drawing on programmatic lessons learned and the tenets of Better Buying Power (BBP) 3.0, we are structuring processes and tailoring our acquisition methodologies to ensure we retain the leading edge.

### Cyber Operations

Nowhere is the need for a proactive approach more pressing than in cybersecurity, where threats must be countered in hours rather than in months or years. While the Army cannot predict the future or design a "silver bullet"

**Fahey** *is executive director for System of Systems Engineering and Integration in the U.S. Army's office of the Assistant Secretary for Acquisition, Logistics and Technology. He is a member of the Senior Executive Service and previously was the Program Executive Officer for Combat Support and Combat Service Support and Program Executive Officer for Ground Combat Systems.*




to block all attacks, we are implementing a flexible strategy to adapt and change. Our goal is to bend the acquisition paradigm to meet cyber requirements, which will ensure that soldiers and systems are equipped to prevent, counter and recover from cyber attacks.

Cybersecurity and other cyber operations pose unique challenges that typically fall outside the normal process lines for requirements, acquisition and resourcing. For this reason, the Army is looking at optimizing existing processes in all three areas in order to be more responsive to cyber requirements and emerging threats while implementing BBP. We have worked diligently to streamline system updates, testing and certification processing to ensure that warfighting capabilities are resilient to the current cyber threat, and we are focused on keeping the edge through innovative approaches to technology insertions.

For example, the Assistant Secretary of the Army for Acquisition, Logistics and Technology, or (ASA[ALT]), is establishing a cyber industry consortium and utilizing the existing Army Venture Capital Initiative for market research to find companies with niche cyber capabilities that can be quickly transitioned to Army programs. Developmental pilot programs and Science and Technology initiatives also allow the ASA(ALT) to better define cyber requirements and identify technology that is adaptive to the ever-changing threat environment.

## Commercial Innovation

As with cyber capabilities, information technology (IT) proliferates faster than traditional Army processes can keep up. As the Army continues to modernize its tactical communications network to enable a more agile and expeditionary force, we are leveraging commercial innovation to retain overmatch.

For example, we mimicked the in-flight Internet services provided by the major airlines by installing high-bandwidth antennas on C-17 aircraft, which will enable the Global Response Force to plan missions with uninterrupted voice, data and video connectivity from garrison to theater. Working in conjunction with the National Security Agency, we adapted the security software used for online shopping to deliver secure wireless and 4G LTE (Long Term Evolution) access inside Army command posts.

Commercial innovation also can be built directly into our contract structure. Just as today's smartphones undergo hardware refreshes every few years to support the newest operating system, Army radio hardware must evolve continuously in parallel with waveform software. With that in mind, the Army has implemented a competitive approach that aims to lower costs and deliver radios more quickly using Non-Developmental Item products. The strategy—grounded in BBP principles—includes frequent competitions among multiple vendors for mature radios that are compatible with government waveforms. This "radio marketplace" will drive innovation in areas like weight, power and battery life while maintaining interoperability between different vendor systems—allowing the Army to incrementally provide soldiers with better radios as these become available on the market.

But the need for agility goes beyond IT. The Joint Light Tactical Vehicle (JLTV), which will fill the gap between the legacy High Mobility Mutlipurpose Wheeled Vehicle ("Humvee") and the bulkier, less mobile Mine Resistant Ambush Protected (MRAP) vehicle, is using a commercial off-the-shelf-based acquisition strategy and adaptive approach to lower costs and incorporate improvements over the program's life cycle.

Among other applications of BBP, program managers incorporated mission command network integration into the early vehicle design. This will allow the Army to make future upgrades to the JLTV much more quickly and cheaply than the equivalent efforts today, when we find ourselves spending more on vehicle integration kits and power upgrades for communications systems than on the new systems themselves.

## Standards Enable Future Solutions

The concept of planning for technology insertions early in a program's life cycle applies to both hardware and software. To set the conditions for future upgrades, the Army is putting in place the standards to enable "plug-and-play" insertion of new capabilities on existing platforms. Consistent with BBP, the creation of such standards encourages competition among a wide pool of potential competitors to lower the cost of integrated technology solutions. There are countless everyday examples of successful standards within which innovation can flourish, ranging from the consistent interfaces of the U.S. power grid to the largely open architecture of the Android mobile ecosystem.

The Army is actively pursuing standards on several fronts. We are moving to publish detailed guidance this year on how government and industry partners will comply with the Modular Open Systems Architecture, which outlines design principles and interface characteristics allowing for modular hardware

and software components to be removed and replaced easily, as needed. Compliance also is progressing with the VICTORY effort, in which the standards are aimed at commonality in electronic interfaces between vehicles and their systems for communications and electronic warfare. VICTORY, which stands for "Vehicle Integration for C4ISR/EW [Communications, Computers, Intelligence, Surveillance, Reconnaissance/Electronic Warfare] Interoperability," is replacing the "bolt-on" approach to fielding equipment on Army vehicles with a more strategic, open architecture approach that makes upgrades easier and more cost effective. Now transitioning into several platforms across the Army's vehicle fleet, the VICTORY architecture will improve integrated situational awareness for mounted soldiers while saving significant space, weight and power.

Standards for software also are moving forward with the phased implementation of the Common Operating Environment (COE). Reaching from mobile handhelds to the tactical cloud, the COE transforms how soldiers can access and share information on the battlefield. Not only does it provide a consistent user experience across different systems and devices—much like what soldiers see on their own smartphones, tablets and laptops at home—the COE also simplifies the way soldiers share information across systems and echelons. For example, the task of moving graphics from brigade to battalion to company down to a platoon leader previously required crossing at least three different systems, all with different designs and standards. That forces units to create workarounds that are often time-consuming and prone to user error. With the COE's "system of systems" interoperability standards, those barriers between echelons are eliminated, enabling a more seamless flow of information.

While the COE requires the Army to invest in improved infrastructure—such as high-performing servers that can do the work previously performed by multiple machines—the overall hardware footprint will significantly decrease as stovepiped mission command systems are replaced by integrated web applications. These apps will share the same map engine, chat function, and secure underlying data, decreasing training time for soldiers while increasing agility for an expeditionary force. Consolidating existing capabilities as part of the COE will also lead to efficiencies in testing, fielding and sustainment.

To encourage competition and innovation, the COE provides software development kits enabling industry and other third parties to contribute new tactical applications to the standard baseline. Using the BBP framework, the Army is examining different methods to create a competitive contracting environment that will allow us to quickly procure and insert these technologies as needed to meet evolving missions.

## Conclusion

The advantages of leveraging commercial technology are obvious: The Army spends less on development and gets capabilities to the field faster. Doing that smartly—so we safeguard security, promote competition and ensure "plug and play" interoperability among evolving technologies—is more complicated.

With BBP as the foundation, we are moving forward with an adaptive, standards-based approach that will affordably address emerging threats and drive innovation to sustain technological dominance—today and into the future.

*The author can be contacted at* **kevin.m.fahey2.civ@mail.mil**.